

Postal services — DPM infrastructure — Messages supporting DPM applications

ICS 03.240

National foreword

This Draft for Development is the official English language version of CEN/TS 15130:2005.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

A review of this Draft for Development will be carried out not later than 2 years after its publication.

Notification of the start of the review period, with a request for the submission of comments from users of this Draft for Development, will be made in an announcement in the appropriate issue of Update Standards. According to the replies received, the responsible BSI Committee will judge whether the Draft for Development can be converted into a British Standard or what other action should be taken.

Observations which it is felt should receive attention before the official call for comments will be welcomed. These should be sent to the Secretary of BSI Technical Committee SVS/4, Postal services, at British Standards House, 389 Chiswick High Road, London W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

A list of organizations represented on this subcommittee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

Summary of pages

This document comprises a front cover, an inside front cover, the CEN/TS title page, pages 2 to 44, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 May 2006

© BSI 2006

ISBN 0 580 48340 1

Amendments issued since publication

Amd. No.	Date	Comments

English Version

**Postal services - DPM infrastructure - Messages supporting
DPM applications**

Postalische Dienstleistungen - Schnittstelle für
Elektrotechnische Signatur

This Technical Specification (CEN/TS) was approved by CEN on 7 May 2005 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36 B-1050 Brussels

Contents		Page
Foreword.....		3
Introduction		4
1	Scope	5
2	Normative references	6
3	Terms and definitions	6
4	Requirements	10
5	Description of the models (system architecture and interaction diagrams)	14
Annex A (normative) Implicit certification process.....		38
Annex B (normative) Message structure.....		40
Annex C (informative) Development principles.....		43
Bibliography		44

Foreword

This document (CEN/TS 15130:2006) has been prepared by Technical Committee CEN/TC 331 “Postal Services”, the secretariat of which is held by NEN.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this CEN Technical Specification: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

Introduction

The purpose of this document is to define a consistent and complete set of messages between vendors and posts infrastructures in support of DPM applications.

It is assumed that the reader of this document is familiar with computer-related technologies normally used to design and implement applications requiring an interaction between computer systems. This document makes use of industry-accepted technical standards and concepts like public key cryptography and communication protocols.

This document defines the significant content and the format for data exchanges and messages, consistent with current industry practices. Also, consistent with the concepts of extensibility and flexibility, this document allows for extensions supporting specific (local) implementations using additional data elements.

1 Scope

This document specifies the information exchanges between various parties' infrastructures that take place in support of DPM applications. It complements standards that address the design, security, applications and readability of Digital Postage Marks.

The following items will be addressed by this document:

- identification of parties participating in exchanges of information described by this document;
- identification of functions (interactions, use cases);
- definition of parties' responsibilities in the context of above functions;
- definition of messages between parties: message meaning and definition of communication protocols to support each function;
- definition of significant content (payload) for each message;
- security mechanisms providing required security services, such as authentication, privacy, integrity and non-repudiation.

This document does not address:

- design of DPM supporting infrastructure for applications internal to providers and carriers;
- design of DPM devices and applications for applications internal to end-users.

NOTE Although there are other communications between various parties involved in postal communications, this document covers only DPM-related aspects of such communications.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, or references to a version number, only the edition cited applies. For undated references and where there is no reference to a version number, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9798-3, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*

ISO 10126-2, *Banking – Procedures for message encipherment (wholesale) – Part 2: DEA algorithm*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

- 3.1 ascending register value**
numerical value that is equal to the total accumulated value of postage that has been accounted for and printed by the mailing system (usually used in the context of a postage meter or a franking machine)
- 3.2 authentication**
verification of the identity of a person, process or the origin of the data being exchanged
- 3.3 control sum**
sum of the descending register value and ascending register value in a mailing system
- 3.4 cryptographic material**
information used in conjunction with cryptographic methods of protecting information
- 3.5 cryptographic key**
information that uniquely determines a bijection (one-to-one transformation) from the space of messages to the space of ciphertexts
- 3.6 Cryptographic Validation Codes**
CVC
value, cryptographically derived from selected postal data, which may be used in verifying the integrity of such data and authenticating its origin
- 3.7 data integrity**
property of a communication channel whereby data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source
- 3.8 descending register value**
numerical value equal to the total value of unused postage remaining in the mailing system (usually used in the context of a postage meter or a franking machine)

3.9**Digital Postage Mark**

DPM

postmark printed or otherwise attached to a mail item and containing information that may be captured and used by mail handling organizations and the recipient

3.10**DPM signature verification key**

public key that is used for the DPM signature verification

3.11**DPM signing Key**

DPM signature generation key

private key that is used for digital signing of DPM information

3.12**DPM verifier**

verifier

postal equipment that is used for DPM verification

3.13**Exchange Validation Codes**

EVC

code, known to or agreed between a mailer and a licensing post, which when applied to a postal item by the mailer may be used by the licensing post to authenticate the origin of the item and, under appropriate circumstances, to verify the integrity of agreed upon DPM data

3.14**implicit certificate**

informational element that binds an entity's identity with its public cryptographic key allowing the verification of the digital signature by another entity using only information contained within the certificate itself

NOTE In Digital Postage Mark verification systems based on public key cryptographic schemes, the verification key is public and can either be retrieved from a database (explicit certificate) or it can be computed from the information contained in the Digital Postage Mark (implicit certificate).

3.15**key management infrastructure**

systems, policies and procedures used to create, store, distribute and update cryptographic keys

3.16**license**

formal permission to account for postal charges and create an agreed upon evidence of payment for such charges given to qualified mailers by posts, carriers or their authorised agents

3.17**license number**

informational element (typically numeric or alphanumeric code) that represents the fact that a mailer has obtained license from the post or a carrier authorising the mailer to account for postal charges and to print evidence of a paid postage

3.18**licensing post**

postal organisation responsible for issuing licenses to qualified mailers

3.19

MAC key

DPM MAC key

Message Authentication Code (MAC) key used for the protection of the Digital Postal Mark (DPM) in DPM systems based on symmetric key cryptographic schemes

3.20

mailer

person or organization using the services of a post

3.21

mailing system

system which is used to account and evidence charges for postal services

NOTE Variations of a mailing system include:

- franking machine or postage meter;
- personal computer with specialized software;
- on-line software service

3.22

Message Authentication Code

MAC

value, cryptographically derived from selected data, which allows data integrity and implicit data origin to be verified

NOTE Since MACs are based on shared secret schemes they allow for weaker (implicit) data origin verification than digital signatures that are based on public key cryptographic schemes.

3.23

non-repudiation

security service which prevents an entity from denying previous commitments or actions

3.24

parametrisation

process of supplying a system or a device with all input information required for proper operation, involving assignment of specific numerical values to named variables used in computation of output values such as data elements of DPM

3.25

post

postal administration

postal authority

organization which has been designated by the UPU member country or territory as an operator responsible for fulfilling part or all of the member's obligations arising from adherence to the UPU convention and agreements

3.26

postal code

numeric or alphanumeric value that is uniquely indicative of a geographic location of an element of postal processing and delivery network, including postal processing facilities, retail offices, delivery units and individual recipient's mailboxes

3.27

privacy

confidentiality

security service used to keep the (meaningful) content of the information from all but those authorised to have it

3.28**public key cryptography**

cryptographic system that uses two keys: a public key accessible to all parties and a private or secret key known only to one party (either the sender or the recipient of the message depending on the use of the system)

NOTE An important element of the public key system is that the public and private keys are uniquely related to each other and it is computationally infeasible to compute private key from the knowledge of public key.

3.29**Public Key Infrastructure****PKI**

system of digital certificates, certificate authorities, and registration authorities or agents that allows for authentication of all parties involved in communication and data exchange processes

3.30**symmetric key cryptography**

encryption system in which the sender and receiver of a message share a single, common secret information (key) that is used both to encrypt and decrypt messages that are being exchanged

3.31**time stamp**

value of the current time stored by a system to indicate when a certain transaction took place

3.32**Universal Coordinated Time****UCT**

universal time, taking into account the addition or omission of leap seconds by atomic clocks each year to compensate for changes in the rotation of the earth (Greenwich Mean Time updated with leap seconds)

3.33**vendor**

provider and/or operator of mailing systems

3.34**World Wide Web Consortium****W3C**

international consortium of companies involved with the development of open standards for internet and the web

3.35**XML**

Extensible Mark-up Language

subset of SGML constituting a particular text mark-up language for interchange of structured data

3.36**XML schema**

XML schema is an XML language for describing and constraining the content of XML documents

4 Requirements

4.1 Functional structure

This clause covers the organization of the logical layer of communication between post and vendor.

In the context of this document, a typical postal operator or a carrier of physical mail items is organized along well-defined functional elements. Specifically, typical functional elements are postal operations (including: mail collection, processing, sorting, transportation and delivery) and system administration and management control (including finance and marketing).

Since this document defines (for the major part) communications between vendor and post aimed at supporting postal revenue collection based on DPM, the postal operator is the main recipient and beneficiary of the information collected and communicated within the DPM supporting infrastructure.

Therefore, the functional requirements are organized to match the functional elements of the postal organization namely: postal operations and system administration and management control. Accordingly, Clause 5 of the present document is organized into the following major subclauses:

- key management processes;
- licensing and parameterization of mailing systems;
- data collection and reporting processes;
- audit-related process.

In this organization, key management processes support postal operations while licensing and parameterization, data collection and audit-related clauses support system administration and management control.

Postal revenue collection systems that are based on DPM require postal verification of accounting processes performed by mailers. In practice, this amounts to DPM verification that is performed on individual mail items and, as such, becomes a part of postal operations.

DPM verification requires that all verification equipment (verifiers) have access to DPM verification keys or key materials (symmetric or public).

For the purpose of this document these verification keys are supplied to verifiers from postal key management infrastructure. The postal key management infrastructure in its relation to vendor key management infrastructure is covered in subsequent clauses of this document.

4.2 Technical requirements

Technical requirements for this document are driven by the needs of posts and vendors to create and operate a cost-effective, functional and efficient infrastructure which allows them to exchange information as described in Clause 5.

This infrastructure will allow interoperability between systems owned and operated by vendors and posts eliminating the need for custom interfaces between specific parties. The use of established technologies and industry-standard solutions will minimize the cost of such infrastructure. The optimum set of solutions is highly dependent on specific conditions and the state of the technology at any given time.

Specific performance levels (like scalability, speed, reliability, availability) are outside the scope of this document, as they evolve quickly and they vary greatly between organizations.

Annex B includes as an example a specific implementation of the transport layer using XML schema standard for data representation.

4.3 Security requirements

4.3.1 General

This subclause is a review of security requirements which are of specific interest to posts and vendors, in the context of DPM infrastructure. It includes a discussion of threats, vulnerabilities and approaches to reduce risks.

4.3.2 Introduction

This clause defines security requirements for the DPM supporting infrastructure and in its general approach follows Annex C "Security analysis considerations" of EN 14615. 4.3.4 defines threats and countermeasures that are specific to DPM supporting infrastructure.

Security of the Digital Postage Marks (DPM) rests on the information present in the DPM, and on security of DPM supporting infrastructure. The DPM information is designed to convince a verifier after it captures and interprets it that the postal charge accounting for the mail piece has occurred and that the payment has been made or will be made (depending on the payment arrangement). The basic principle at work here is the notion that certain information can be known to a mailer's postage evidencing device only if it has access to a protected (secret or private) piece of information known as a key. Access to such key shall always trigger an accounting action that results in a secure accounting for the postal charge (amount) required to be paid for the service of postal delivery. This secure accounting is performed either by deduction of the computed postage amount from an accounting register (descending register) responsible for storage of pre-paid funds or simply by updating a secure non-volatile register (ascending register) by the computed amount or both. Thus the DPM security and its linkage to a payment mechanism are delivered through secure cryptographic information processing using a private (secret) key. It is of paramount importance that such keys be securely managed throughout their use within the system. This document deals with DPM key management system and its specific arrangements concerning vendor-post interface.

A cryptographic system normally requires a clear definition of the message sender, message communication channel, message recipient and the message itself. For the purpose of this document both vendor and post play roles of sender and recipient since they engage in exchange of vital information required for the proper functioning of a DPM-based payment system. Such exchange is organised by using a public or private communication network that is referred to as a communication channel. In the process of exchanging required information vendor and post execute an agreed upon communication protocol normally consisting of a several rounds of sending and receiving information.

The usual services of information security are entity or message data origin authentication, message data integrity, message data confidentiality (privacy) and sender non-repudiation (see Bibliography [2] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14])

4.3.3 Security business objectives, policy and economics

This subclause defines most important security business objectives, policy and economics. Other more detailed security objectives, policy and economics are application and environment dependent and typically can be derived from the objectives listed below:

- a) postal business objective is to create and maintain cost effective access to postal services for mailers without negative impact on the quality of service and its ease of use. Specifically, postal revenue collection including DPM infrastructure security measures shall be balanced against the cost of implementation and maintenance of secure DPM supporting Infrastructure. This shall be done in such a way that the overall combined cost of revenue collection including the cost that shall be incurred by post, vendor and their joint customers is minimal;
- b) fundamental security policy and economics requirement is that a postal revenue collection system does not allow for attacks (resulting in significant revenue losses) that are easy to mount for dishonest mailers or outside participants and are difficult to detect and protect against for post and vendor. The qualifications "easy" and "difficult" here are understood in economic terms. "Easy" means that material,

human and timing resources required to mount an attack are relatively low compared with potential economic rewards for a successful attack. "Difficult" means that those required resources are relatively high compared to potential rewards. Similarly, countermeasures implemented by vendor and post are "easy" if they require comparatively low resources for successful detection of an attack and result in identification and prosecution of perpetrators. Countermeasures that require comparatively large resources are considered "difficult". More specifically, there are several fundamental security policy requirements, namely: 1) the postal accounting systems/devices manufactured and distributed by vendor shall accurately account for postal funds, 2) the postal accounting systems/devices shall provide all necessary information for verification of postage payment, 3) the payment verification systems shall be able to detect postal fraud, identify responsible party or parties and support evidence collection and prosecution of responsible party or parties and 4) the design of vendor and post infrastructures supporting DPM shall not allow for "easy" attacks that do not have effective countermeasures (defined as countermeasures that require small material, human and timing resources);

- c) legal framework shall be developed that defines legal recourse against perpetrators of postal fraud in the digital environment together with required standards of evidence. The legal framework for DPM infrastructure environment is outside of the scope of this document.

4.3.4 Threats and vulnerabilities (attacks)

Threats correspond to methods of attacking a system with the objective of causing damage to it, its operators or users. Actual attacks may combine several such methods.

The approach taken in this document is to define only threats and vulnerabilities that are specific to DPM supporting infrastructure and avoid definition and description of attacks common to all digital communication systems.

The remainder of this clause is devoted to the identification and brief description of a number of threats that are specific to DPM supporting infrastructure:

- a) **collusion** involves cooperation between two or more parties with fraudulent intent. It may occur between mailers, between a mailer and a supplier (vendor), or between one of these and a corrupt postal employee. For example, an individual employed by one mailer may assist another mailer to generate mail purporting to originate in his own organization, or a mailer may bribe a postal employee to gain access to protected information such as key and key material. Collusion attacks can not be totally prevented but at a minimum postal audit of vendor and mailing system as well as DPM verification processes will support the detection of collusion;
- b) **cryptanalysis** is the use of mathematical techniques in an attempt to defeat the use of cryptographic methods, particularly in the context of information security services. It is normally aimed at the recovery of cryptographic keys by exploiting knowledge of the cryptographic algorithm, data that forms input to and/or output from the algorithm, or both. DPM infrastructure design and communication protocols employed in the vendor-post interface described in this document make use of public and symmetric key cryptographic primitives. This document generally avoids making specific recommendations concerning precise use and type of cryptographic primitives within key management, data collection and reporting, licensing, parameterization and audit procedures. For the purpose of this document it is sufficient to describe all covered protocols and procedures using generic nomenclatures such as public or symmetric key schemes and thus leaving the choice of specific primitives to qualified designers of the DPM supporting infrastructure. However, it is strongly recommended that only well-known and tested cryptographic primitives such as RSA, DSA, ECDSA, Triple DES and AES be used as primitives in the procedures described in this document. Specific choice of cryptographic primitives should be guided by computational, interoperability and IT constraints as well as other system requirements known to exist in country-specific systems.

Recommended implementations of proven cryptographic primitives are described in appropriate ISO, CEN, ANSI and other national standards and are outside of the scope of this document;

- c) **illegitimate key access** covers access to the secret cryptographic key or keys of a legitimate device or user by an unauthorized party, thereby allowing the party concerned to masquerade (cryptographically) as the legitimate device or user. Illegitimate access to cryptographic keys puts at risk any cryptographically protected features of the system. A properly designed DPM infrastructure system prevents such access by requiring a sound key management and protection system as described in this document;
- d) **Information Technology (IT) system infiltration** covers the range of threats that are common to IT systems. All of the issues associated with IT system infiltration are addressed in separate documents and are not covered by this document since they are not specific to DPM infrastructure. However, several classes of threats that are of particular interest in the design, implementation and administration of DPM supporting infrastructure are briefly described. It is strongly advised that designers of DPM supporting infrastructure systems review, assess and implement technical and administrative countermeasures appropriate for their specific IT systems:
- 1) **network tampering** covers a range of threats that are both passive and active attacks on communications channels. Network tampering attacks may be conducted on public networks, such as the internet, or private networks, such as a vendor or post's internal network. Monitoring of network traffic and data in order to gain access to confidential information is a passive attack that may be accomplished using freely available network administration tools. Active attacks include injecting data into a communications channel and modifying data on a communications channel. Injecting data involves inserting additional traffic into a communication channel. The traffic may be a replay of prior data or newly constructed data. The purpose of injecting data may be to gain access to services (e.g. replaying an authorization to increase the postage value resident in a mailing system) or to deny services (e.g. to overwhelm a server with data thereby denying service to others). Modifying data involves changing the content of data sent via a communication channel before the intended recipient receives the data (e.g. increasing a credit limit);
 - 2) **unauthorized database and server modification** covers the range of threats that involve unauthorized access to computers and databases that implement an IT System in order to modify the server or database. The access may be local (e.g. from a computer keyboard) or remote (e.g. over a computer network). For example, modifying a server configuration could enable the unauthorized viewing of confidential information or the denial of access to authorized parties. Similarly, the modification of data in a database either directly or by restoring a backup of earlier data could be used to change privileges (e.g. a credit limit);
 - 3) **illegitimate long-term storage access** covers the range of threats that involve access and/or modification of archival data (e.g. backup tapes of servers and databases or even paper records). Illegitimate access to archival data could reveal confidential information to unauthorized parties. Unauthorized modification of archival data could be used to obscure evidence of other attacks or facilitate unauthorized database and server modification;
- e) **repudiation** occurs when one of the parties to a transaction denies his or her involvement in it. For example, in a Mailing system management system, the sending of a postage value download to a customer's meter represents the transfer of money. If the customer subsequently claims that the download was never received, the postal administration and/or vendor could lose revenue if it is unable to tie the download transaction to the customer's subsystem (e.g. through an undeniable audit trail or transaction history). Similarly, in a system based on postal administration of postage accounting a mailer could attempt to deny responsibility for the origination of items. Repudiation is addressed in this document where appropriate by the recommended use (within key management, audit and data reporting procedures) of proven digital signature primitives and protocols;
- f) **security system infiltration** is defined as penetration of a security system with the objective of disabling it or reducing its effectiveness. For example, fraudulent DPM public verification key insertion, in which an unauthorised key value is inserted into the set of legitimate verification keys supported by the security system, would jeopardize the integrity of a postal revenue collection system. Similarly, some key management systems recommended in this document and supporting DPMs protected by symmetric key cryptography require internal postal sharing of a single universal DPM verification key between a server and multiple verifiers. Although this document is generally not concerned with post's and vendor's internal